Amendments to the Claims

This listing of claims will replace all prior versions, and listings, of claims in the application:

Listing of Claims:

1. (previously presented): A system for dynamically detecting computer viruses through associative behavioral analysis of runtime state, comprising:

a parameter set stored on a client system defining a group of monitored events, each monitored event comprising a set of one or more actions defined within an object, each action being performed by one or more applications executing within a defined computing environment;

a monitor executing on the client system, comprising:

a collector continuously monitoring runtime state within the defined computing environment for an occurrence of any one of the monitored events in the group and tracking a sequence of execution of the monitored events for each of the applications; and

an analyzer identifying each occurrence of a specific event sequence characteristic of behavior of a computer virus and the application which performed the specific event sequence, creating a histogram describing the specific event sequence occurrence for each of the applications, and identifying repetitions of the histogram associated with at least one object.

2. (original): A system according to Claim 1, further comprising:

a storage manager organizing the histograms into plurality of records ordered by object, application, and monitored event.

3. (original): A system according to Claim 2, further comprising:

a structured database in which the plurality of records is stored; and the storage manager storing each histogram for each such specific event sequence occurrence in one such database record identified by the application by which the specific event sequence was performed.

4. (original): A system according to Claim 3, further comprising:

the storage manager configuring the structured database as an event log organized by each event in the group of monitored events and updating the database record storing each specific event sequence occurrence with a revised histogram as each such occurrence is identified.

5. (original): A system according to Claim 1, further comprising:

the analyzer detecting suspect activities within each histogram, each suspect activity comprising a set of known actions comprising a computer virus signature.

6. (previously presented): A system according to Claim 5, wherein each such suspect activity is selected from a class of actions comprising file accesses, program executions, message transmissions, configuration area accesses, security setting accesses, and impersonations.

7. (currently amended): A system according to Claim [[~~6~~]] 5, wherein each such suspect activity is selected from a group comprising files accesses, program executions, direct disk accesses, media formatting operations, sending of electronic mail, system configuration area accesses, changes to security settings, impersonations, and system calls having the ability to monitor system input/output activities.

8. (previously presented): A system according to Claim 1, wherein the computer virus comprises at least one form of unauthorized content selected from a group comprising a computer virus application, a Trojan horse application, and a hoax application.

9. (previously presented): A method for dynamically detecting computer viruses through associative behavioral analysis of runtime state, comprising:

defining a group of monitored events, each monitored event comprising a set of one or more actions defined within an object, each action being performed by one or more applications executing within a defined computing environment;

continuously monitoring runtime state within the defined computing environment for an occurrence of any one of the monitored events in the group;

tracking a sequence of execution of the monitored events for each of the applications;

identifying each occurrence of a specific event sequence characteristic of behavior of a computer virus and the application which performed the specific event sequence;

creating a histogram describing the specific event sequence occurrence for each of the applications; and

identifying repetitions of the histogram associated with at least one object.

10. (original): A method according to Claim 9, further comprising:

organizing the histograms into plurality of records ordered by object, application, and monitored event.

11. (original): A method according to Claim 10, further comprising:

maintaining a structured database in which the plurality of records is stored; and

storing each histogram for each such specific event sequence occurrence in one such database record identified by the application by which the specific event sequence was performed.

12. (original): A method according to Claim 11, further comprising:

configuring the structured database as an event log organized by each event in the group of monitored events; and updating the database record storing each specific event sequence occurrence with a revised histogram as each such occurrence is identified.

13. (original): A method according to Claim 9, further comprising:

detecting suspect activities within each histogram, each suspect activity comprising a set of known actions comprising a computer virus signature.

14. (previously presented): A method according to Claim 13, wherein each such suspect activity is selected from a class of actions comprising file accesses, program executions, message transmissions, configuration area accesses, security setting accesses, and impersonations.

15. (previously presented): A method according to Claim 13, wherein each such suspect activity is selected from a group comprising files accesses, program executions, direct disk accesses, media formatting operations, sending of electronic mail, system configuration area accesses, changes to security settings, impersonations, and system calls having the ability to monitor system input/output activities.

16. (previously presented): A method according to Claim 9, wherein the computer virus comprises at least one form of unauthorized content selected from a group comprising a computer virus application, a Trojan horse application, and a hoax application.

17. (previously presented): A computer-readable storage medium holding code for dynamically detecting computer viruses through associative behavioral analysis of runtime state, comprising:

defining a group of monitored events, each monitored event comprising a set of one or more actions defined within an object, each action being performed by one or more applications executing within a defined computing environment;

continuously monitoring runtime state within the defined computing environment for an occurrence of any one of the monitored events in the group;

tracking a sequence of execution of the monitored events for each of the applications;

identifying each occurrence of a specific event sequence characteristic of behavior of a computer virus and the application which performed the specific event sequence;

creating a histogram describing the specific event sequence occurrence for each of the applications; and

identifying repetitions of the histogram associated with at least one object.

18. (original): A storage medium according to Claim 17, further comprising:

organizing the histograms into plurality of records ordered by object, application, and monitored event.

19. (original): A storage medium according to Claim 18, further comprising:

maintaining a structured database in which the plurality of records is stored; and

storing each histogram for each such specific event sequence occurrence in one such database record identified by the application by which the specific event sequence was performed.

20. (original): A storage medium according to Claim 19, further comprising:

configuring the structured database as an event log organized by each event in the group of monitored events; and

updating the database record storing each specific event sequence occurrence with a revised histogram as each such occurrence is identified.

21. (original): A storage medium according to Claim 17, further comprising:

detecting suspect activities within each histogram, each suspect activity comprising a set of known actions comprising a computer virus signature.